Raytheon
BBN Technologies

BBN Technologies
10 Moulton Street
Cambridge, MA 02138

2 December 2016

US Navy
Office of Naval Research
One Liberty Center
875 North Randolph Street
Arlington, VA 22203-1995

Delivered via Email to:
richard.t.willis@navy.mil
ravindra.athale@navy.mil
alexander.gorelik@navy.mil
reports@library.nrl.navy.mil
tr@dtic.mil

Contract Number:	N00014-16-C-2069
Proposal Number:	P15030A-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Saikat Guha
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Title of the Project:	COmmunications and Networking with QUantum operationally-Secure Technology for Maritime Deployment (**CONQUEST**)
Contract Period of Performance:	2 September 2016 – 1 September 2019
Total Contract Amount:	$3,663,297
Year 1 Contract Amount:	$1,219,339
Amount of Incremental Funds:	$150,000
Total Amount Expended + Committed Funds (thru 25 November):	$104,544 + $54,750

Attention: Dr. Richard T. Willis
Subject: Quarterly Progress Report
Reference: Section J, Exhibit A: Contract Data Requirements List

In accordance with the reference requirement of the subject contract, Raytheon BBN Technologies (BBN) hereby submits its first Progress Report. This cover sheet and enclosure have been distributed in accordance with the contract requirements.

Please do not hesitate to contact Dr. Saikat Guha at 617.873.5122 (email: saikat.guha@raytheon.com) should you wish to discuss any technical matter related to this report, or contact the undersigned, Ms. Kathryn Carson at 617.873.8144 (email: kathryn.carson@raytheon.com) if you would like to discuss this letter or have any other questions.

Sincerely,
Raytheon BBN Technologies

Kathryn Carson
Program Manager
Quantum Information Processing

CONQUEST Quarterly Progress Report #1 for the Period
2 September 2016 – 1 December 2016 (3 Months)

Section A. Task Progress

Task 1.1: QKD operation and security analysis for a naval atmospheric link with a realistic eavesdropper

The slides attached to this report provide an update regarding Task 1 progress.

Task 2.1: Maritime-implementable QKD protocols

General security proof of discrete-modulation CV QKD

Saikat Guha has been in discussions with Kamil Bradler of CipherQ Corp. on extending the proof technique of Lutkenhaus et al., PRA 79, 012307, which proved security and a rate lower bound for a binary-input (BPSK) CV QKD protocol. The main challenge in extending this proof technique to an M-ary is that this requires us to retain the entire relative "geometry" of the M purifications of the Eve's states (i.e., M choose 2 inner products). We are investigating a way where we could argue that the symmetry of the transmitted ensemble (e.g., a M-ary PSK constellation) is preserved in the symmetry of a particular purification of Eve's conditional states, which lets us proceed with evaluating bounds to conditional entropies using only a few parameters that describe that geometry, and in turn will hopefully lead to a rate lower bound with a simple-to-implement key map that only has a few quantities that Alice and Bob need to estimate during the channel estimation step.

Better post-processing for BPSK CV QKD in lieu of slightly-reduced rate

Saikat Guha and Masahiro Takeoka has been working on the attached draft [BPSK_CVQKD.pdf] -- of work being done in collaboration with Hari Krovi and Norbert Lutkenhaus -- on simple post-processing schemes for BPSK QKD protocols (much smaller communications overhead at the expense of slightly reduced rate, but yet with the optimal linear rate-transmittance scaling), and also a new rate-upper-bound proof that establishes the optimal rate attainable with a 2-state QKD protocol with heterodyne detection.

Task 3: Maximizing the information efficiency of QKD

Floodlight Quantum Key Distribution (FL-QKD): Theory

(1) We have completed an analysis of FL-QKD using K-ary phase-shift keying (K-PSK) and quadrature amplitude modulation (QAM) , thus generalizing from our initial work on binary PSK. For the fiber channel, K-PSK allows the secret-key rate (SKR) against the optimum collective attack, to be doubled, but QAM beyond 4-ary (which is the same as 4-PSK), offers no advantage. A conference paper on this work will be submitted to CLEO 2017 this month, and a journal article is in preparation.

(2) We are continuing to work on the coherent-attack security of FL-QKD and hope to complete a security proof and SKR assessment during the next quarter.

(3) The preceding theory was done for a quiescent channel, e.g., optical fiber. In previous work on another program we have done some analysis of FL-QKD for the atmospheric channel, and we are beginning to extend that work.

Floodlight Quantum Key Distribution (FL-QKD): Experiment

(1) We have previously performed a table-top proof-of-principle FL-QKD experiment that demonstrated a 55 Mbps SKR using 100 Mbps binary PSK on a channel with 10 dB of attenuation (equivalent of 50 km of optical fiber). That experiment's modulation rate (and hence its SKR) were limited by the capabilities of the equipment on hand at that time. We have now acquired the equipment needed to run a table-top experiment at a 10 Gbps modulation rate, and we are proceeding to perform an FL-QKD experiment that should achieve a 1 to 2 Gbps SKR on a channel with 10 dB of attenuation.

(2) We are working to implement a field-programmable gate array (FPGA) implementation for our FL-QKD system's servo control, which will be a great convenience for future experiments.

Task 4: Improved hardware-domain signal processing

Photonic Integrated Circuit Work

We have demonstrated high-speed polarization-encoded QKD using silicon photonic integrated devices. The QKD transmitter is a polarization-dependent Mach-Zehnder modulator designed on a CMOS-compatible silicon-on-insulator photonics platform. The transmitter generates arbitrary polarization qubits at gigahertz bandwidth with an extinction ratio better than 30 dB at 1480 nm using high-speed carrier-depletion phase modulators. We tested the performance of this device in a 104m field test between two different buildings at MIT. The experiment, done with a clock rate of 62.5 MHz, generated secret keys at a rate of 623.3 kbps along with a bit error rate of 1.77% and a phase error rate of 0.67%. We are currently implementing further protocol improvements, such as asymmetric basis selection and faster clock rate, to bring the secret key rate well into the Mbps range. The work shows the potential of using advanced photonic integrated circuits to enable high-speed quantum-secure communications.

Task 5: QKD network via un-trusted quantum nodes

Non-deterministic amplifiers for use as quantum repeaters for CV QKD

Boulat Bash and Saikat Guha are investigating the efficacy of using NLAs for quantum repeaters for CV-QKD -- an idea recently put forth by Tim Ralph and collaborators. We have explicitly evaluated the rate performance afforded by a single NLA repeater station, implemented using the "quantum-scissors" based approach. A detailed calculation has been carried out of the post-selected state at the end between Alice and Bob, and the probability of success associated with that. We have found -- from calculating the reverse coherent information of that heralded entangled state, and accounting for the heralding probability -- that there is no improvement over the TGW bound using this one-station NLA repeater approach. This does not yet prove this does not work, but it suggests we may need either (a) more repeater nodes, or more likely (b) some

form of cross-channel multiplexing, for this to beat the TGW bound. There is no known form of CV QKD quantum repeater that is known to beat the TGW bound (upper bound on the rate of the best direct-transmission QKD protocol). We are working on both of those directions.

Task 6: Important technical issues to address current deficiencies in the theory/practice of QKD

Exploring novel non-Gaussian receivers for CV QKD for better finite-key performance

Saikat Guha and Zachary Dutton have been exploring the performance of the Bondurant receiver for demodulating the coherent-state M-ary PSK alphabet. The Bondurant receiver works using a conditional-nulling strategy, a style of optical receiver implemented by the BBN group earlier [Nature Photonics 6, 374–379 (2012)]. In prior work funded by the InPho program, the BBN team had shown that the generalized Bondurant receiver can attain a factor of 4 improvement in the error probability exponent of demodulating M-ary PSK (or for that matter any M-ary coherent state alphabet). We have now found that that improved demodulation error exponent translates into better finite-length rate performance. We have derived a semi-analytic expression for the full transition matrix of the generalized Type-I Bondurant receiver for demodulating M-ary PSK, and translated that to calculating capacity and dispersion (latter quantifies the finite-length rate). So far, we have completed an analysis of the finite-length rate performance improvement afforded by the generalized Bondurant receiver for classical communication (just the I(A;B) term, not yet the \chi(B;E) term, which in turn will complete the full secret-key rate calculation). We intend to write this up as a paper soon, and then extend the analysis to key rate. We expect that this receiver or some variant of it will improve the finite-key-length performance of discrete modulation CV QKD protocols. Details attached in the short memo.

The LSU team has been investigating finite-energy bounds on QKD protocols. To this end, we had thought a paper of Ryo Namiki would be useful for this purpose since there was a claim that it was possible to use CV teleportation to simulate a pure-loss channel of a lower transmissivity with one having a higher transmissivity. Upon further inspection of Namiki's paper, we found that there is an error and so we are thinking of alternative methods for devising finite-energy bounds.

The LSU team has devised a measure of quantum steering that uses conditional mutual information and which we call intrinsic steerability. We proved several properties of this measure that establish it as a steering monotone. We suspect that it will find applications in one-sided device independent quantum key distribution as a bound on secret key rates achievable in that setting.

Takeoka and the LSU team determined the optimal Fisher information when estimating the excess noise in a thermal channel with a fixed transmissivity. This should be useful for estimation of excess noise in quantum key distribution protocols.

Section B. Planned Activities/Schedule

A program kickoff meeting was held at BBN on October 7th with all team members in attendance. See attached slides from kick-off meeting. Monthly team meetings have been scheduled and the last monthly meeting was held via teleconference on November 23rd. The next scheduled team meeting will be held at MIT on December 15th. BBN's internal team

meetings are scheduled for every other Tuesday morning. For information regarding planned technical activities, see the updates provided in Section A above.

Section C. Equipment Purchased

No equipment has been purchased or constructed at this time.

Section D. Key Personnel

There have been no changes in personnel.

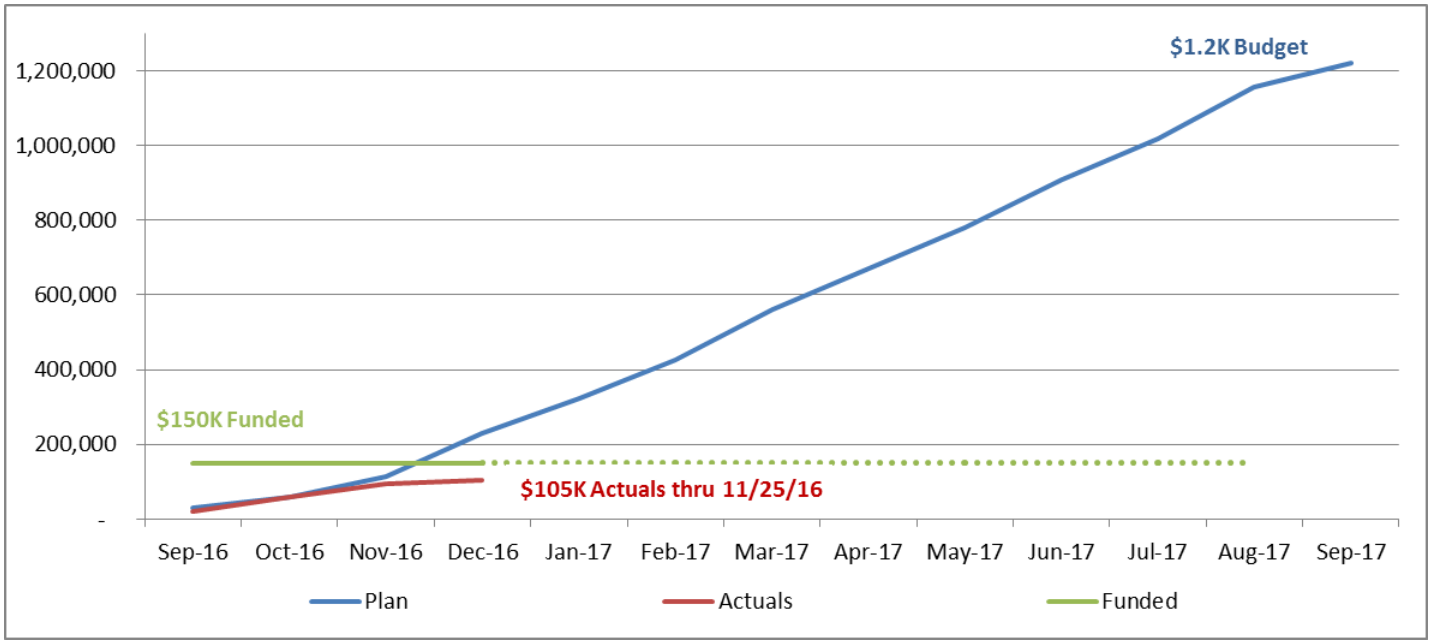
Section E. Accomplishments

See updates provided in Sections A and B above and in both attachments – program slides and two memos – entitled, "Binary modulated CV QKD: simplified post-processing at the expense of small reduction in rate, and optimal post processing that meets rate upper bound" and "Capacities and coding efficiencies for the Sequentual Waveform Nulling with phase shift keying modulation."

Section F. Anticipated Problems

There are no anticipated problems or issues to report at this time.

Section G. YR1 CONQUEST Budget



Binary modulated CV QKD: simplified post-processing at the expense of small reduction in rate, and optimal post processing that meets rate upper bound

Masahiro Takeoka[1], Saikat Guha[2], Hari Krovi[2], and Norbert Lütkenhaus[3]
[1] *National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan*
[2] *Quantum Information Processing Group, Raytheon BBN Technologies, Cambridge, MA 02138, USA*
[3] *Institute for Quantum Computing, University of Waterloo, Waterloo ON, N2L 3G1, Canada*
(Dated: December 1, 2016)

Continuous variable (CV) quantum key distribution (QKD) has a practical advantage in its implementation since it can use conventional optical telecom components, and does not require cryostats to support good-quality single photon detectors required for discrete variable QKD protocols. On the other hand, one of CV QKD's practical drawbacks is the highly complicated signal modulation and classical post processing of the output of the heterodyne detector, and the associated low transmission ranges due to electrical noise bandwidth limitations of the detector. In this paper, we extend the binary phase shift keyed (BPSK) CVQKD protocol investigated in Zhao et al., Phys. Rev. A **79**, 012307 (2009) in two ways. First, we show that the post processing protocol described in the above paper is optimal in the sense that it achieves the secret-key-generation capacity (with unlimited two-way public authenticated communication) of a pure-loss bosonic channel under the constraints of the BPSK coherent-state alphabet and heterodyne detection. Second, we propose a suite of simplified post processing protocols which attain slightly suboptimal key rate performance while greatly reducing the cost of post processing and classical communication.

I. INTRODUCTION

Quantum key distribution (QKD) is a protocol to share secret key between two distant parties Alice and Bob such that the key is provably secure against an eavesdropper, Eve, who has unlimited eavesdropping technology allowed by quantum mechanics. QKD is now not only with a scientific interest but also emerging as a practical technology and has been implemented in the field testbeds around the world [1–4].

Many of the QKD protocols rely on single photon detector [5] which is technically a hard part and often limits the practical performance and cost of the system. Alternative protocols are called continuous variable QKD (CVQKD) where the information from Alice is encoded in the quadrature of optical field and is detected by quadrature measurements such as homodyne or heterodyne detectors at Bob's side. The practical advantage of CVQKD is that their detectors are commonly used in conventional optical communication and thus one can use off-the-shelf technologies developed in that field. On the other hand, the drawbacks are complications of the quantum signal modulation and the classical postprocessing. A standard CVQKD protocol, known as the GG02 protocol [6], uses coherent state modulated in phase space with continuous Gaussian distribution which is more complicated than the discrete modulations used in other QKD protocols. In addition, the measured data is also continuously distributed which should be properly discretized and processed at the classical postprocessing step. This makes another complication (mostly at error correction) in practical systems.

Another practical problem is the data length at the key distillation step. In single photon detection based QKD, photon detection probability at Bob is proportional to the channel transmittance, which is very small for long distance channels. Since only the photon detected outcomes are distilled for the final key generation, the amount of data used at the key distillation is much smaller than the number of pulses originally sent from Alice. In CVQKD on the other hand, since the detection outcomes are continuous values of quadratures, all of the measured outcomes must be used for the distillation process. This makes the distillation process of CVQKD more complicated than that of the single photon detection based QKDs.

One possibility to overcome these techinical issues is to consider discretely modulated CVQKD using for example binary phase shift keyed (BPSK) modulation [7–9]. The reason that Gaussian modulation is more commonly used than the discrete modulation is of its security aspect. Since discretely modulated signal ensembles has non-Gauissian statistics, the security proof of the discretly modulated CVQKD becomes nontrivial and complicated. However, regardless of this complication, the lower bound of the achievable key rate against collective attacks for the BPSK modulation has been shown for a pure-loss channel [8] and later for general channels [9].

In this paper, we extend the BPSK CVQKD protocol proposed in [8, 9] and further investigate its postprocessing part toward establishing the QKD protocol benefiting all the above practical advantages. More precisely, we pursue the QKD protocol with the minimum postprocessing cost whereas keeping the merits of off-the-shelf optical technologies and simple signal modulation format. Figure 1 summarizes the steps of the classical postprocessing of the BPSK CVQKD in [9]. After measuring the quantum signals and storing continuous variable measurement outcomes, Alice and Bob do channel estimation by usnig a part of the data and then sifting the keys (if necessary).

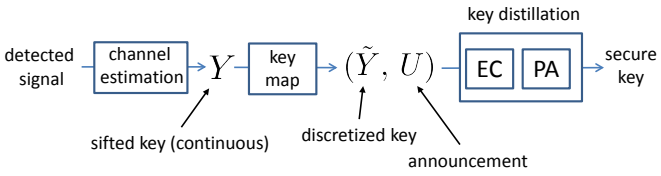


FIG. 1: Classical postprocessing in continuous variable quantum key distribution. EC: error correction. PA: privacy amplification.

The sifted key Y is then mapped to two variables $\tilde{Y}$ and U where the former is the discretized data used for the key distillation and the latter is publically announced to Alice which contributes to increase the mutual information (and thus the final key rate) between Alice and Bob. Throughout the paper, we refer the process $Y \to (\tilde{Y}, U)$ as the *key map*.

Our paper has two main contributions. First, we prove that the key map in Zhao et al.'s protocol [9] is optimal in the sense that it achieves the capacity of a pure-loss bosonic channel under constraint of the physical setting of the BPSK CVQKD. In addition, as a minor result, we propose the "efficient" version of Zhao et al.'s protocol by using the idea of the efficient protocol proposed for BB84 protocol [10]. This protocol can improve the key rate and also does not require active switching of the detectors. Second, we propose simpler key maps reducing the cost of classical processing and communication whereas keeping suboptimal key rate performance in a pure-loss bosonic channel. We believe the results contribute a way toward developing a provably secure CVQKD protocol taking the advantages of optical communication components, simple signal modulation, and simple classical postprocessings.

II. EFFICIENT BPSK-CVQKD PROTOCOL

In this section, we revisit the BPSK-CVQKD protocol proposed in [8, 9] and consider its "efficient" version. We consider only the asymptotic limit of the inifnitely long key exchanges. Alice picks a binary-valued random variable $X \in \{0, 1\}$ with equal probabilities, and transmits one of the two BPSK coherent state pulses $|\alpha_x\rangle_A \in \{|-\alpha\rangle, |\alpha\rangle\}$, $x = 0, 1$, with $\alpha \in R$, $|\alpha|^2 = \bar{n}$ to Bob through the quantum channel. While Bob's receiver is assumed to be a heterodyne receiver in [9], we replace it with the *asymmetric* heterodyne receiver meaning that the signal pulse is split via an asymmetric (non-50/50) beamsplitter with transmittance $\eta_{\rm BS} > 0.5$ and then the real quadrature of the transmitted signal and the imaginary quadrature of the reflected signal are measured by homodyne detectors. This asymmetric detection is similar to the idea of the "efficient" protocol in BB84 [10] and contributes to gain the key rate. In the limit of infinitely long pulse sequence, the channel estimation is possible even taking $\eta_{\rm BS} \to 1$.

Let Y be the strings of the sifted key, i.e. the measurement outcome of the real quadrature after sifting the signals used for channel estimation. After the channel estimation, Bob performs the key map which maps a string of y to announcement u and discretized key $\tilde{y}$. The announcement is publically announced to Alice to help her key distillation process. Then Alice and Bob do the error correction and the privacy amplification to distill the key from $(X, \tilde{Y})$ conditioned on U. The key map particularly considered in [9] is $u = |y|$ and $\tilde{y}$ is the sign of y which we call the infinite discretized key map.

In the following, we consider a specific scenario such that the channel is estimated to be a pure-loss channel with transmittance $\eta \in (0, 1]$. In addition, we assume that the quantum devices in Alice and Bob's sides do not have any imperfection and also they can perform ideal error correction and privacy amplification. Two reasons for choosing this scenario: 1) it simplifies the key rate analysis, and more importantly, 2) in a pure-loss channel, we can prove the optimality of the infinite discretized key map in the sense that it achieves the capacity of the efficient BPSK-CVQKD protocol in this channel. The rigorous statement of the capacity and its proof will be given in Sec. IV.

In the limit of $\eta_{\rm BS} \to 1$ with the above assumption, the conditional probability of Bob's measurement outcome y is given by $p(y|X = 0) \equiv p(y|0) = \frac{1}{\sqrt{\pi}} e^{-(y-\sqrt{2\eta\bar{n}})^2}$ and $p(y|X = 1) \equiv p(y|1) = \frac{1}{\sqrt{\pi}} e^{-(y+\sqrt{2\eta\bar{n}})^2}$. Under these assumptions, the key rate lower bound against collective attacks with the infinite discretized key map is obtained from [9] by taking zero excess noise. It is given by

$$R^{(\infty)} \geq \int_0^\infty dy\, f(y) \left[1 - h(\epsilon_y) - h\left(\frac{1+\kappa}{2}\right) + h\left(\frac{1+\sqrt{1-4\epsilon_y(1-\epsilon_y)(1-\kappa^2)}}{2}\right)\right], \quad (1)$$

where $f(y) \equiv p(y|0) + p(y|1)$, $\epsilon_y = \frac{p(y|0)}{p(y|0)+p(y|1)} = \frac{1}{1+e^{4\sqrt{\eta\bar{n}}|y|}}$, and $\kappa = e^{-2(1-\eta)\bar{n}}$. The key rate in (1) maximized over $\bar{n}$ gives the achievable rate of the BPSK-CVQKD with the infinite discretized key map. With this key map, Bob ideally announces the continuous value $u = |y|$ to Alice via a public channel which costs additional classical information transmission. In practice, $|y|$ should be discretized. The amount of classical information for U is therefore approximately given by m bits/pulse for 2^m discretization.

As we mentioned, the key rate in Eq. (1) is indeed the capacity of the efficient BPSK-CVQKD in a pure-loss channel, that is, the infinite discretized key map is the best strategy to maximize the key rate under the fixed physical setup of the efficient BPSK-CVQKD.

III. SIMPLIFIED KEY MAPS

In this section, we propose two simplified key maps for the BPSK-CVQKD. Although the infinite discretized key map is optimal for maximizing the key rate, the cost for the classical processing and communication could be large since the announcement U should be continuous variable in ideal. Our simplified key maps can reduce the classical cost significantly whereas keeping the suboptimality of the achievable key rates. Again, for simplicity, we calculate the achievable key rate under the assumptions that the quantum channel between Alice and Bob is estimated to be a pure-loss channel and Eve's attacks are restricted to be collective attacks. The key rate calculation for each key map is along with [9] which we describe in detail in Appendix for completeness.

A. 2-bin discretized key map

Bob makes a hard decision, based on the sign of y, to obtain, $\tilde{Y} \in \{0,1\}$ and does not send any announcement to Alice (i.e. $U \in \{\emptyset\}$). $\tilde{Y}$ is interpreted as an output of a binary symmetric channel $BSC(\epsilon)$ with X as the input where $\epsilon = \int_0^\infty p(y|0)dy = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\eta\bar{n}}\right)$. The lower bound of the key rate is given by

$$R^{(2)} \geq 1 - h(\epsilon) - h\left(\frac{1+\kappa}{2}\right) + h\left(\frac{1+\sqrt{1-4\epsilon(1-\epsilon)(1-\kappa^2)}}{2}\right), \quad (2)$$

where $\kappa = \exp[-2(1-\eta)\bar{n}]$ and $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy function. This rate is maximized over $\bar{n}$ for each given η. Since $U \in \{\emptyset\}$, Bob can fully save the classical communication cost for the announcement.

B. 3-bin discretized protocol

Next simplest is the 3-bin discretization. Bob makes a two-step decision: first assign $U = \{0,1\}$ for $\{|y| \geq \delta_{\mathrm{th}}, |y| < \delta_{\mathrm{th}}\}$ where δ_{th} is a positive threshold parameter, and $u = 1$ is regarded as a failure outcome. That is, by the announcement, Bob tells Alice success or failure for each pulse which costs 1 bit/pulse. For each success event, Bob assigns $\tilde{y} = \{0,1\}$ for negative and positive y, respectively, and use it to distill the final keys. The key rate is thus a function of the success probability $P_{\mathrm{succ}} = \frac{1}{2}\left(2 + \mathrm{erf}\left(\sqrt{\eta\bar{n}} + \delta_{\mathrm{th}}\right) - \mathrm{erf}\left(\sqrt{\eta\bar{n}} - \delta_{\mathrm{th}}\right)\right)$ and is given by

$$R^{(3)} \geq P_{\mathrm{succ}}\left[1 - h(\tilde{\epsilon}) - h\left(\frac{1+\kappa}{2}\right) + h\left(\frac{1+\sqrt{1-4\tilde{\epsilon}(1-\tilde{\epsilon})(1-\kappa^2)}}{2}\right)\right], \quad (3)$$

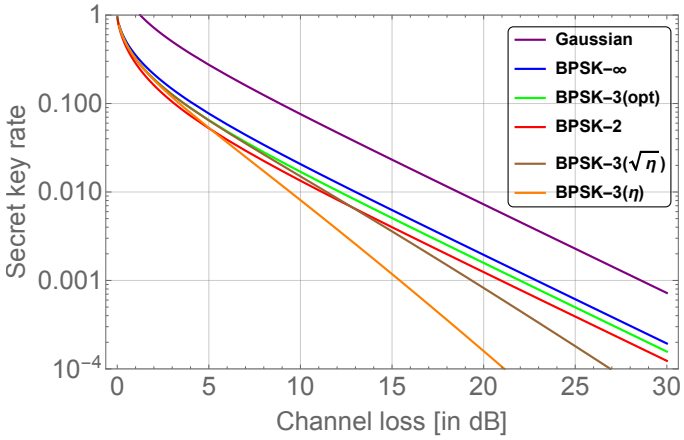


FIG. 2: Key rates for various CV QKD protocols.

where

$$\tilde{\epsilon} = \frac{1 - \mathrm{erf}\left(\sqrt{\eta\bar{n}} + \delta_{\mathrm{th}}\right)}{2 + \mathrm{erf}\left(\sqrt{\eta\bar{n}} - \delta_{\mathrm{th}}\right) - \mathrm{erf}\left(\sqrt{\eta\bar{n}} + \delta_{\mathrm{th}}\right)}. \quad (4)$$

Again, the above key rate is maximized over $\bar{n}$ for each given η. In this key map, we have a freedom to choose δ_{th}. In the following, we consider three options: 1) optimize δ_{th} such that the key rate is maximized for each gievn η, 2) choose δ_{th} such that P_{succ} is equal to η and 3) choose δ_{th} such that P_{succ} is equal to $\sqrt{\eta}$. The idea of the second option is to mimic the success probability of the single-photon based protocols such as BB84 which could significantly reduce the classical communication and processing cost for the key distillation. The third option is in between 1) and 2).

In summary, the classical communication cost for the announcement is 1 bit/pulse (success or failure information) and that for the key distillation depends on the choice of δ_{th}.

C. Key rate comparison

Figure 2 plots the key rates as a function of channel loss for 2-bin, 3-bin, and infinite discretized key maps. Also for comparison, the standard CVQKD protocol with Gaussian modulation and actively switched homodyne detection also plotted [5, 6] (see also [11] for a summarized key rate expression). There are several observations. First, scaling of all the key rates except the 3-bin discretized key maps with $P_{\mathrm{succ}} = \eta$ and $\sqrt{\eta}$ are $O(\eta)$. This is known to be the optimal rate-loss scaling for any point-to-point QKD protocols in a pure-loss channel [11–13]. Second, the key rate gap between the Gaussian CVQKD and the efficient BPSK-CVQKD with the infinite discretized key map is relatively small (factor of 3.7 for small η). As mentioned in the introduction, the efficient BPSK-CVQKD has practical advantages compared to the Gaussian-CVQKD such as simple

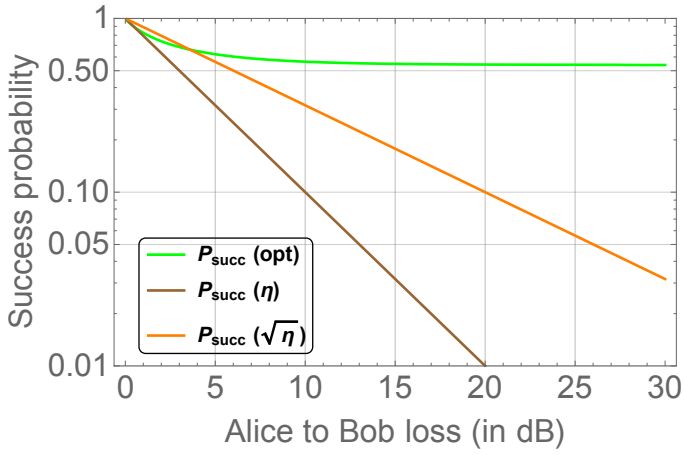


FIG. 3: Success probabilities of the 3-bin discretized key maps with different thresholds.

modification and non-necessity of active switching at detection. Third, moreover, the rate degradation by the simplification of the key map from infinite to 2 or 3-bin discretizations in the BPSK-CVQKD is rather small (less than factor of 1.6) whereas the announcement cost is zero (2-bin) or 1 bit/pulse (3-bin). These observations show the potential of the BPSK-CVQKD with the simple key maps as classical cost effective protocols.

For the 3-bin discretized key map, it is observed that the reduction of the success probability clearly decreases the key rate scaling. In other words the plots show the trade-off between the key rate scaling and the classical data cost at the key distillation step. In the straight line region, the key rates roughly scales as $O(\eta^{1.7})$ and $O(\eta^{1.3})$ for $P_{\text{succ}} = \eta$, and $\sqrt{\eta}$, respectively. The length of $\{\tilde{y}\}$ processed at the key distillation step depends on the success probability at the key map. In Fig. 3, we plot the success probabilities for the different 3-bin key maps. Even though the rate scaling reduces for lower success probabilities, Figs. 2 and 3 still suggest the usefulness of the non-optimal 3-bin key map. For example, comparing the 3-bin key map with $P_{\text{succ}} = \sqrt{\eta}$ by the inifinite discretized key map at 20dB losses, the key rate of the former is 42% of the latter whereas the length of $\tilde{y}$ to be distilled for the former reduces to only 6% of the latter. That is, with the 3-bin key map with $P_{\text{succ}} = \sqrt{\eta}$, while the obtainable key rate reduces to 2/5 of the best key rate in the efficient BPSK CVQKD, one can compress the necessary data length for the key distillation less than 1/16 of the original signal length n.

IV. PROOF OF THE UPPER BOUND

In this section we provide a rigorous proof of the optimality of the infinite discretized key map. The precise statement of our capacity theorem is as follows.

Theorem 1 *The secret key capacity of the lossy bosonic channel of transmissivity η, under constraint of (a) BPSK coherent state transmission of mean photon number $\bar{n}$, and (b) asymmetric heterodyne measurement used at the receiver, is given by:*

$$C_s^{\text{BPSK}} = \int_0^\infty dy\, f(y) \left[1 - h(\epsilon_y) - h\left(\frac{1+\kappa}{2}\right) + h\left(\frac{1+\sqrt{1-4\epsilon_y(1-\epsilon_y)(1-\kappa^2)}}{2}\right)\right], \quad (5)$$

where $f(y) \equiv p(y|0) + p(y|1)$ and $\epsilon_y = \frac{p(y|0)}{p(y|0)+p(y|1)} = \frac{1}{1+e^{4\sqrt{\eta\bar{n}}|y|}}$.

Proof. Due to the constraints (a) and (b), after the transmission of the BPSK signals and detection via an asymmetric heterodyne receiver with $\eta_{\text{BS}} \to 1$, Alice, Bob, and Eve share copies of *ccq*-state:

$$\rho_{XYE} = \sum_x \int_{-\infty}^{\infty} dy\, p_X(x) p_{Y|X}(y|x) |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes |\gamma_x\rangle\langle\gamma_x|_E, \quad (6)$$

where $X \in \{0,1\}$, Y is a continuous variable with $p_{Y|X}(y|0) = \frac{1}{\sqrt{\pi}} e^{-(y-\sqrt{2\eta\bar{n}})^2}$ and $p_{Y|X}(y|1) = \frac{1}{\sqrt{\pi}} e^{-(y+\sqrt{2\eta\bar{n}})^2}$, and $\gamma_x \in \{\pm\sqrt{1-\eta}\alpha\}; x = 0,1$. Also it is easy to show that $p_X(0) = p_X(1) = 1/2$ maximizes the key rate. Thus the secret key capacity corresponds to the maximum key rate extractable from copies of ρ_{XYE}.

The achievability is already shown in (1). To prove the converse, we use the intrinsic information quantity which was shown to be an upper bound to the maximum extractable key rate from i.i.d. multiple copies of a tripartite shared quantum state ρ_{ABE} [14].

$$I(A;B\downarrow E)_\rho \equiv \inf I(A;B|E')_\rho, \quad (7)$$

where $I(A;B|E')_\rho$ is the quantum conditional mutual information of state $\rho_{ABE'}$ and the infimum is taken over all completely positive trace preserving maps $\Lambda_{E\to E'}$ from E to E' where $\rho_{ABE'} = (I_{AB} \otimes \Lambda_{E\to E'})(\rho_{ABE})$. We may choose the map $\Lambda_{E\to E'}$ as the identity operation, to give us a (potentially loose) upper bound.

Then applying it to our ρ_{XYE} in Eq. (6), we get the upper bound of the secret key capacity as

$$\begin{aligned} C_s^{\text{BPSK}} &\le I(X;Y|E)_\rho \\ &= H(XE)_\rho + H(XE)_\rho - H(XYE)_\rho - H(E)_\rho, \end{aligned} \quad (8)$$

where $H(X)_\rho$ is the von Neumann entropy of the state ρ_X. ρ_{XE}, ρ_{XE}, ρ_E are the reduced density matrices of ρ_{XYE}. The reduced density matrices and the von Neumann entropies are calculated as follows:

$$\begin{aligned} \rho_{YE} &= \sum_x \int_{-\infty}^{\infty} dy\, p_X(x) p_{Y|X}(y|x) |y\rangle\langle y| \\ &= \int_0^\infty dy\, f(y) |y\rangle\langle y|_Y \\ &\quad \otimes \{\epsilon_y |\gamma_0\rangle\langle\gamma_0| + (1-\epsilon_y)|\gamma_1\rangle\langle\gamma_1|\}_E, \end{aligned} \quad (9)$$

where $f(y) = p_{Y|X}(y|0) + p_{Y|X}(y|1)$ and $\epsilon_y = \frac{p_{Y|X}(y|0)}{p_{Y|X}(y|0)+p_{Y|X}(y|1)}$, which implies

$$H(YE)_\rho = H(Y)_\rho + \int_0^\infty dy\, f(y) \times h\left(\frac{1+\sqrt{1-4\epsilon_y(1-\epsilon_y)(1-\kappa^2)}}{2}\right), \tag{10}$$

where $\kappa^2 = |\langle\gamma_0|\gamma_1\rangle|^2 = e^{-4(1-\eta)\bar{n}}$. Similarly,

$$\rho_{XE} = \frac{1}{2}(|0\rangle\langle 0|_X \otimes |\gamma_0\rangle\langle\gamma_0|_E + |1\rangle\langle 1|_X \otimes |\gamma_1\rangle\langle\gamma_1|_E), \tag{11}$$

leading to:

$$H(XE)_\rho = h(1/2) = 1. \tag{12}$$

Similarly,

$$\rho_E = \frac{1}{2}(|\gamma_0\rangle\langle\gamma_0|_E + |\gamma_1\rangle\langle\gamma_1|_E), \tag{13}$$

leading to:

$$H(E)_\rho = h\left(\frac{1+\kappa}{2}\right). \tag{14}$$

Finally,

$$H(XYE)_\rho = 1 + H(Y)_\rho. \tag{15}$$

Substituting these into Eq. (8), we obtain the upper bound

$$C_s^{\mathrm{BPSK}} \leq \int_0^\infty dy\, f(y)\left[1 - h(\epsilon_y) - h\left(\frac{1+\kappa}{2}\right) + h\left(\frac{1+\sqrt{1-4\epsilon_y(1-\epsilon_y)(1-\kappa^2)}}{2}\right)\right], \tag{16}$$

which coincides with the lower bound, thereby completing the proof. ■

V. CONCLUSIONS

In this paper, we extend the BPSK CVQKD protocol proposed in [8, 9] and investigate the minimum postprocessing cost whereas keeping the merits of off-the-shelf optical technologies and simple signal modulation format of the BPSK CVQKD. Frist, we have proved that the key map in Zhao et al.'s protocol [9] is optimal in the sense that it achieves the capacity of a pure-loss bosonic channel under constraint of the physical setting of the BPSK CVQKD. Also, we propose the "efficient" version of Zhao et al.'s protocol as a CVQKD version of the efficient BB84 protocol proposed in [10]. This protocol can improve the key rate while not requiring active switching of the detectors. As a second contribution, we have proposed simpler key maps, the 2-bin and 3-bin discretized key maps, and show that they keep suboptimal key rate performance in a pure-loss bosonic channel while reducing the cost of key map and annoucement in classical post processing. In addition, we point out that in the 3-bin discretized key map, it is even possible to reduce the classical communication cost for the error correction and privacy amplification step which has been one of the technical drawbacks in CVQKD. We show a tradeoff between the key generation rate and the failure probability of the key map where the latter contributes to reduce the data length for the error correction and privacy amplification. Depending on the channel and other technical conditions, one can design appropriate threshold for the key map.

The results shown here are useful toward developing a CVQKD protocol taking the advantages of optical communication components as well as simple signal modulation and classical postprocessings. The remaining important task is to develop a security proof and tight key rate lower bound applicable to arbitrary quantum channel.

Acknowledgement

SG and HK would like to acknowledge support from the ONR CONQUEST program, and a subcontract from Sandia National Laboratories under the SECANT-QKD program.

[1] Chip Elliott. Building the quantum network. *New Journal of Physics*, 46:1–12, 2002.

[2] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J. F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legrè, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Robyr, L Salvail, A. W Sharpe, A. J Shields, D Stucki, M Suda, C Tamas, T Themel, R. T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z. L Yuan, H Zbinden, and A Zeilinger. *New Journal of Physics*, 11.

[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Mat-

sui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387–10409, 2011. arXiv:quant-ph/1103.3566.

[4] Shuang Wang, Wei Chen, Zhen-Qiang Yin, Hong-Wei Li, De-Yong He, Yu-Hu Li, Zheng Zhou, Xiao-Tian Song, Fang-Yi Li, Dong Wang, Hua Chen, Yun-Guang Han, Jing-Zheng Huang, Jun-Fu Guo, Peng-Lei Hao, Mo Li, Chun-Mei Zhang, Dong Liu, Wen-Ye Liang, Chun-Hua Miao, Ping Wu, Guang-Can Guo, and Zheng-Fu Han. Field and long-term demonstration of a wide area quantum key distribution network. *Optics Express*, 22(18):21739, sep 2014.

[5] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Review of Modern Physics*, 81:1301–1350, 2009. arXiv:0802.4155.

[6] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88:057902, 2002.

[7] Ch. Silberhorn, T C Ralph, N Lütkenhaus, and G Leuchs. Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit. *Phys. Rev. Lett.*, 89:167901, 2002.

[8] Matthias Heid and Norbert Lütkenhaus. Efficiency of coherent-state quantum cryptography in the presence of loss: influence of realistic error correction. *Physical Review A*, 73:052316, 2006.

[9] Yi Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A - Atomic, Molecular, and Optical Physics*, 79(1):1–14, 2009.

[10] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and proof of its unconditional security. *Journal of Cryptography*, 18:133–165, 2005. arXiv:quant-ph/0011056.

[11] Masahiro Takeoka, Saikat Guha, and Mark M Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature communications*, 5:5235, jan 2014.

[12] Masahiro Takeoka, Saikat Guha, and MM Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, 2014.

[13] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. 2015. arXiv:1510.08863.

[14] Matthias Christandl, Artur Ekert, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Renato Renner. Unifying classical and quantum key distillation. *Proceedings of the 4th Theory of Cryptography Conference, Lecture Notes in Computer Science*, 4392:456–478, February 2007. arXiv:quant-ph/0608199.

[15] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72(1):012332, jul 2005.

[16] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461:207–235, 2005.

Appendix: Achievable key rates for the efficient BPSK-CVQKD with the 2-bin and 3-bin discretized key maps

In this appendix, we describe detailed derivation of the key rate lower bound for the efficient BPSK-CVQKD with 2-bin, and 3-bin key maps.

Our security analysis follows the one in [9] based on [15, 16], but assuming a pure-loss bosonic channel. As usual, we consider the (virtual) entanglement protocol in which Alice prepares the entangled state $\frac{1}{\sqrt{2}}(|0\rangle_A|-\alpha\rangle_{A'} + |1\rangle_A|\alpha\rangle_{A'})$ and then sends system A' to Bob through a quantum channel $A' \to B$. We assume that Eve can make any purification on the state shared by Alice and Bob, which we denote as ψ_{ABE}.

In the asymptotic limit of long key length, the secret key generation rate R against any collective attacks is lower bounded by [9],

$$R \geq I(X;\tilde{Y}|U) - \max_{\psi_{ABE}} I(\tilde{Y};E|U)_\rho, \qquad \text{(A.1)}$$

where $\tilde{Y} \in 0, 1$ is the sign of y measured by Bob which cotains the information about Alice's BPSK encoding, U is some information announced from Bob to Alice (and Eve) via a public channel. The second term is a quantum conditional mutual information for the *ccq* state

$$\begin{aligned} \rho_{U\tilde{Y}E} &\equiv \mathrm{Tr}_A\left[\mathcal{M}_{B\to U\tilde{Y}}\left(\psi_{ABE}\right)\right] \\ &= \sum_{u,\tilde{y}} p(u,\tilde{y})|u\rangle\langle u|_U \otimes |\tilde{y}\rangle\langle\tilde{y}|_{\tilde{Y}} \otimes \rho_E^{u\,\tilde{y}}, \end{aligned} \qquad \text{(A.2)}$$

where $\mathcal{M}$ includes Bob's asymmetric heterodyne measurement $B \to Y$ and the key map $Y \to U\tilde{Y}$.

Suppose Bob obtains the distribution $p(y|X=0) \equiv p(y|0) = \frac{1}{\sqrt{\pi}}e^{-(y-\sqrt{\eta}\alpha)^2}$ and $p(y|1) = \frac{1}{\sqrt{\pi}}e^{-(y+\sqrt{\eta}\alpha)^2}$ at the channel estimation step. This specifies that Bob's conditional states before the measurement are $|\pm\sqrt{\eta}\alpha\rangle\langle\pm\sqrt{\eta}\alpha|$. Thus the purification held by Alice, Bob, and Eve should have the following form:

$$|\Psi\rangle_{ABE} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|-\sqrt{\eta}\alpha\rangle_B|\phi_-\rangle_E + |1\rangle_A|\sqrt{\eta}\alpha\rangle_B|\phi_+\rangle_E\right). \qquad \text{(A.3)}$$

where Bob and Eve's systems should preserve the inner product of the signal sent from Alice:

$$|\langle-\alpha|\alpha\rangle| = |\langle-\sqrt{\eta}\alpha|\sqrt{\eta}\alpha\rangle\langle\phi_-|\phi_+\rangle|. \qquad \text{(A.4)}$$

This implies that

$$\begin{aligned} |\langle\phi_-|\phi_+\rangle| &= |\langle-\sqrt{1-\eta}\alpha|\sqrt{1-\eta}\alpha\rangle| \\ &= \exp[-2(1-\eta)\bar{n}] = \kappa, \end{aligned} \qquad \text{(A.5)}$$

where $\bar{n} = |\alpha|^2$. These observations uniquely characterize the optimal purification.

Also, the conditional state of (A.3) on Bob's heterodyne measurement is

$$|\Psi^y\rangle_{AE} = \frac{1}{\sqrt{2\pi^{1/2}p(y)}}\left(e^{-(\sqrt{\eta}\alpha+y)^2/2}|0\rangle_A|\phi_-\rangle_E + e^{-(\sqrt{\eta}\alpha-y)^2/2}|1\rangle_A|\phi_+\rangle_E\right), \quad (A.6)$$

where

$$p(y) = \frac{1}{2}\left(p(y|0)+p(y|1)\right) = \frac{1}{2\sqrt{\pi}}\left(e^{-(\sqrt{\eta}\alpha+y)^2}+e^{-(\sqrt{\eta}\alpha-y)^2}\right). \quad (A.7)$$

1. 2-bin discretized key map

For the 2-bin discretized key map, the effective channel including a quantum channel, Bob's measurement, and the key map is simply given by a classical binary symmetric channel with error $\epsilon = \frac{1}{2}\mathrm{erfc}(\sqrt{\eta\bar{n}})$. Since there is no announcement from Bob, the first term of (A.1) is

$$I(X;\tilde{Y}|U) = I(X;\tilde{Y}) = 1-h(\epsilon). \quad (A.8)$$

For the second term of (A.1), we need to derive Eve's state conditioned on Bob's outcome $\tilde{y}$. From (A.6) we obtain the *cq*-state held by Bob and Eve as

$$\tilde{\Psi}^{(2)}_{\tilde{Y}E} = \sum_{\tilde{y}=0}^{1} p_{\tilde{Y}}(\tilde{y})|\tilde{y}\rangle\langle\tilde{y}|_{\tilde{Y}}\otimes\tilde{\Psi}^{\tilde{y}}_E = \frac{1}{2}\left(|0\rangle\langle 0|_{\tilde{Y}}\otimes\tilde{\Psi}^0_E + |1\rangle\langle 1|_{\tilde{Y}}\otimes\tilde{\Psi}^1_E\right), \quad (A.9)$$

where $p_{\tilde{Y}}(0) = \int_{-\infty}^{0} dy\, p(y) = 1/2$,

$$\tilde{\Psi}^0_E = 2\int_{-\infty}^{0} dy\, p(y)\Psi^y_E = \frac{1}{\sqrt{\pi}}\int_{-\infty}^{0} dy\,\left(e^{-(\sqrt{\eta}\alpha+y)^2}|\phi_-\rangle\langle\phi_-|_E + e^{-(\sqrt{\eta}\alpha-y)^2}|\phi_+\rangle\langle\phi_+|_E\right) = \frac{1+\mathrm{erf}(\sqrt{\eta}\alpha)}{2}|\phi_-\rangle\langle\phi_-|_E + \frac{1-\mathrm{erf}(\sqrt{\eta}\alpha)}{2}|\phi_+\rangle\langle\phi_+|_E, \quad (A.10)$$

and similarly

$$\tilde{\Psi}^1_E = \frac{1-\mathrm{erf}(\sqrt{\eta}\alpha)}{2}|\phi_-\rangle\langle\phi_-|_E + \frac{1+\mathrm{erf}(\sqrt{\eta}\alpha)}{2}|\phi_+\rangle\langle\phi_+|_E. \quad (A.11)$$

These allow us to calculate the necessary entropies:

$$I(\tilde{Y};E|U)_{\tilde{\Psi}^{(2)}} = I(\tilde{Y};E)_{\tilde{\Psi}^{(2)}} = H(E)_{\tilde{\Psi}^{(2)}} - H(E|\tilde{Y})_{\tilde{\Psi}^{(2)}} = h\left(\frac{1+\kappa}{2}\right) - h\left(\frac{1+\sqrt{1-4\epsilon(1-\epsilon)(1-\kappa^2)}}{2}\right), \quad (A.12)$$

where κ is in (A.5) and $\epsilon = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\eta\bar{n}}\right)$. Then from (A.8) and (A.12), we have a desired result.

2. 3-bin discretized key map

The 3-bin discretized key map includes failure events with probability $1-P_{\mathrm{succ}}$ where $P_{\mathrm{succ}} = \frac{1}{2}\left(2+\mathrm{erf}\left(\sqrt{\eta\bar{n}}+\delta_{\mathrm{th}}\right)-\mathrm{erf}\left(\sqrt{\eta\bar{n}}-\delta_{\mathrm{th}}\right)\right)$. The effective channel of a quantum channel and Bob's measurement is then modeled by a binary earsure channel with a symmetric error

$$\tilde{\epsilon} = \frac{1-\mathrm{erf}\left(\sqrt{\eta\bar{n}}+\delta_{\mathrm{th}}\right)}{2+\mathrm{erf}\left(\sqrt{\eta\bar{n}}-\delta_{\mathrm{th}}\right)-\mathrm{erf}\left(\sqrt{\eta\bar{n}}+\delta_{\mathrm{th}}\right)}. \quad (A.13)$$

The conditional mutual information between Alice and Bob is then calculated to be

$$I(X;\tilde{Y}|U) = P_{\mathrm{succ}}\left(1-h(\tilde{\epsilon})\right). \quad (A.14)$$

After Bob's measurement and key map, Bob and Eve hold the following *ccq*-state:

$$\tilde{\Psi}^{(3)}_{U\tilde{Y}E} = p_U(0)|0\rangle\langle 0|_U\otimes\left(p_{\tilde{Y}}(0)|0\rangle\langle 0|_{\tilde{Y}}\otimes\tilde{\Psi}^{\tilde{y}=0}_E + p_{\tilde{Y}}(1)|1\rangle\langle 1|_{\tilde{Y}}\otimes\tilde{\Psi}^{\tilde{y}=1}_E\right) + p_U(1)|1\rangle\langle 1|_U\otimes|2\rangle\langle 2|_{\tilde{Y}}\otimes\tilde{\Psi}^{u=1}_E, \quad (A.15)$$

where

$$p_U(0) = \int_{-\infty}^{-\delta_{\mathrm{th}}} dy\, p(y) + \int_{\delta_{\mathrm{th}}}^{-\infty} dy\, p(y) = \frac{1}{2}\left(2+\mathrm{erf}\left(\sqrt{\eta\bar{n}}+\delta_{\mathrm{th}}\right)-\mathrm{erf}\left(\sqrt{\eta\bar{n}}-\delta_{\mathrm{th}}\right)\right) \equiv P_{\mathrm{succ}}, \quad (A.16)$$

$p_U(1) = 1-P_{\mathrm{succ}}$, $p_{\tilde{Y}}(0) = p_{\tilde{Y}}(1) = 1/2$,

$$\tilde{\Psi}^{\tilde{y}=0}_E = \frac{2}{P_{\mathrm{succ}}}\int_{-\infty}^{-\delta_{\mathrm{th}}} dy\, p(y)\Psi^y_E = \frac{1}{2P_{\mathrm{succ}}}\left\{(1+\mathrm{erf}(\sqrt{\eta\bar{n}}-\delta_{\mathrm{th}}))|\phi_-\rangle\langle\phi_-|_E + (1-\mathrm{erf}(\sqrt{\eta\bar{n}}+\delta_{\mathrm{th}}))|\phi_+\rangle\langle\phi_+|_E\right\}, \quad (A.17)$$

and similarly,

$$\tilde{\Psi}_E^{\tilde{y}=1} = \frac{1}{2P_{\rm succ}}\left\{(1-\mathrm{erf}(\sqrt{\eta\bar{n}}-\delta_{\rm th}))|\phi_-\rangle\langle\phi_-|_E + (1+\mathrm{erf}(\sqrt{\eta\bar{n}}+\delta_{\rm th}))|\phi_+\rangle\langle\phi_+|_E\right\}. \quad \text{(A.18)}$$

Then we have the conditional entropies:

$$H(E|U)_{\tilde{\Psi}^{(3)}} = P_{\rm succ}H(E|u=0)_{\tilde{\Psi}^{(3)}} + (1-P_{\rm succ})H(E|u=1)_{\tilde{\Psi}^{(3)}}, \quad \text{(A.19)}$$

$$H(E|U\tilde{Y})_{\tilde{\Psi}^{(3)}} = \frac{P_{\rm succ}}{2}\left(H(E|u=0,\tilde{y}=0)_{\tilde{\Psi}^{(3)}} + H(E|u=0,\tilde{y}=1)_{\tilde{\Psi}^{(3)}}\right) + (1-P_{\rm succ})H(E|u=1)_{\tilde{\Psi}^{(3)}}, \quad \text{(A.20)}$$

and thus the second term of (A.1) turns out to be

$$I(\tilde{Y};E|U)_{\tilde{\Psi}^{(3)}} = H(E|U)_{\tilde{\Psi}^{(3)}} - H(E|U\tilde{Y})_{\tilde{\Psi}^{(3)}} = P_{\rm succ}\left(h\left(\frac{1+\kappa}{2}\right) - h\left(\frac{1+\sqrt{1-4\tilde{\epsilon}(1-\tilde{\epsilon})(1-\kappa^2)}}{2}\right)\right). \quad \text{(A.21)}$$

Combining Eqs. (A.14) and (A.21), we get the desired result.

Capacities and coding efficiencies for the Sequentual Waveform Nulling with phase shift keying modulation

Zachary Dutton and Saikat Guha
Quantum Information Processing Technologies group,
Raytheon BBN Technologies, Cambridge, MA 02138
(Dated: December 2, 2016)

We calculate the complete error transfer matrix for a sequentual waveform nulling (SWN) receiver applied to communication link with M-ary phase shift keying modulation. We use this to calculate the capacity and dispersion as a function of mean photon number per pulse, which in tern gives us the coding efficiency of the SWN. The results are compared with heterodyne detection as well as the optimal Helstrom measurement. As expected, we find the reduced error rate of the SWN yields a slightly improved capacity than heterodyne when considering envelope defined by all possible M. The dispersion comparison between different receivers is non-trivial as a function of power per pulse, though the SWN recveiver shows a clear advantage over heterodyne in the useful operational range of $1 < N_0 < 10$.

Bondurant [1] first proposed a receiver capable of beating the error rate of coherent detection with a 4-PSK alphabet, based on a sequential nulling strategy in which a LO mixes with the signal to null out the $m = 0$ modulation waveform, and then successfully nulls $m = 1, 2, \ldots$ as single photon clicks are recorded. This strategy was generalized in for any alphabet [2]. Here we focus on the case of an aribtrary MPSK alphabet utilizing the same strategy as Bondurant's original proposal.

In particular we analyze the error rate for $M = 2, 4, 8, 16$ and calculate the complete error transfer matrix. Assuming M possible waveforms, equally spaced in phase and labelled $m = 0, 1, 2, \ldots M-1$. Upon obtaining l clicks over the course of pulse detection, the SWN receiver will guess l. The transition matrix elements, in the absence of dark counts, are $P(l|m) = 0$ for all$l > m$. For $l < m$:

$$P(l|m) = \int_{t_1=0}^{T} P_m(t_1)dt_1 \int_{t_2=t_1}^{T} P_{m-1}(t_2 - t_1)dt_2 \cdots \int_{t_l=t_{l-1}}^{T} P_{m+1-l}(t_l - t_{l-1})dt_l \int_{t_{l+1}}^{\infty} P_{m-l}(t_{l+1} - t_l)dt_{l+1} \quad (1)$$

where $P_k(t) = \lambda_k e^{-\lambda_k t}$ and $\lambda_k = (2N_0/T)[1 - \cos(2\pi k/M)]$. Here N_0 is the mean photon number per pulse and T is the pulse length. And finally for $l = m$:

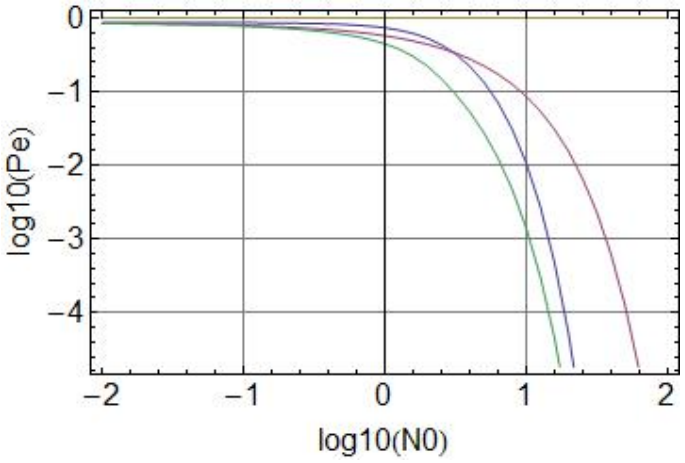


FIG. 1: Error rate versus mean photon number for $M = 8$ for the SWN receiver (blue), and compared with heterodyne (red) and Helstrom limit (green).

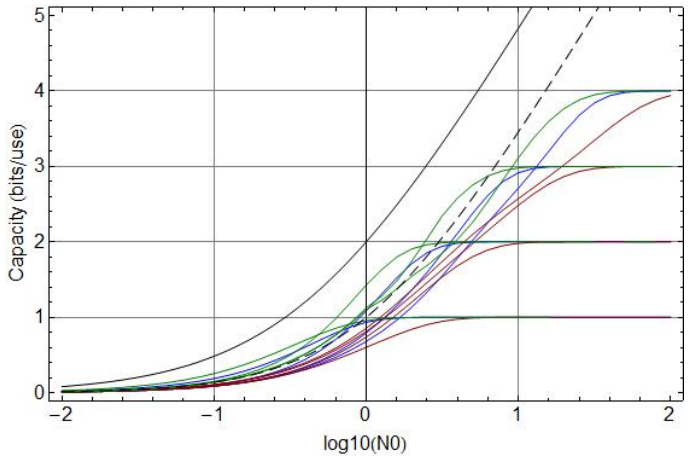


FIG. 2: Shannon capacities of the SWN (blue), Heterodyne (red) and Helstrom limited (green) receivers for $M = 2, 4, 8$, and 16. The dashed curve shows the Heterodyne limit for an unconstrained modulation format $log_2(1 + N_0)$ while the solid black curve shows the Holevo bound.

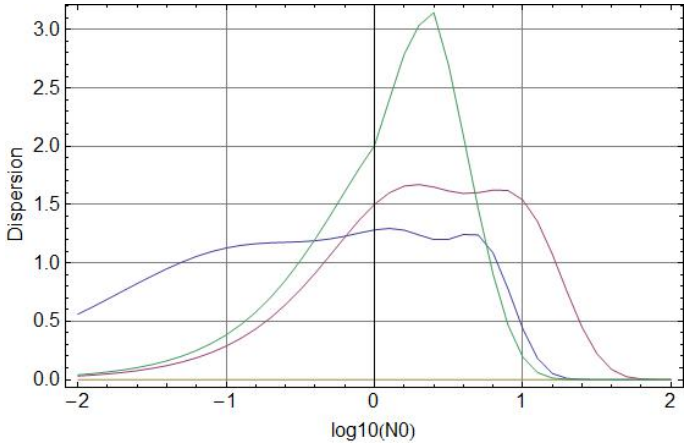


FIG. 3: Dispersion of the SWN (blue), Heterodyne (red) and Helstrom limited (green) receivers for $M = 8$.

$$P(m|m) = \int_{t_1=0}^{T} P_m(t_1)dt_1 \int_{t_2=t_1}^{T} P_{m-1}(t_2 - t_1)dt_2 \cdots \int_{t_m=t_{m-1}}^{T} P_1(t_m - t_{m-1})dt_m \tag{2}$$

This transition matrix can be used firstly to calculate the receiver error rate. The results for $M = 8$ are plotted in Fig. 1. The results for heterodyne and the Helstrom limit. One sees, as expected that as the photon number N_0 increases, the SWN receiver beats heterodyne and scales as the Helstrom limit. It actually performs worse thatn heterodyne at low photon number, with a cross over between 1 and 10 photons. Secondly, we use the transition matrix to calculate the Shannon capacities. We plot the cases $M = 2, 4, 8, 16$ in Fig. 2. Each receiver, as N_0 increases asymptotically approach $\log_2(M)$. We see that the envelope of the SWN receivers exceeds the heterodyne case and even exceeds the unconstrained heterodyne limit below(the dashed curve) $N_0 < 10$. Above this point using a QAM modulation format becomes optimal - though we'd expect the SWN applied to this modulation would maintain its advantage.

Finally, the dispersion is calculated using the same transition matrices. The results for $M = 8$ are plotted in Fig. 3. For dispersion, a lower value means a lower variance in error rate which allows coding with shorter block lengths. One sees the the SWN and heterodyne recievers experience a cross over just below $N_0 < 1$, above which the SWN is superior. The capacity for a finite block length code can be calculated as $C - \sqrt{V/n}\text{Erfc}^{-1}(2\epsilon)$, where $\text{Erfc}^{-1}(x)$ is the inverse complementary error function and ϵ is the targeted error rate. Two examples are shown in 4.

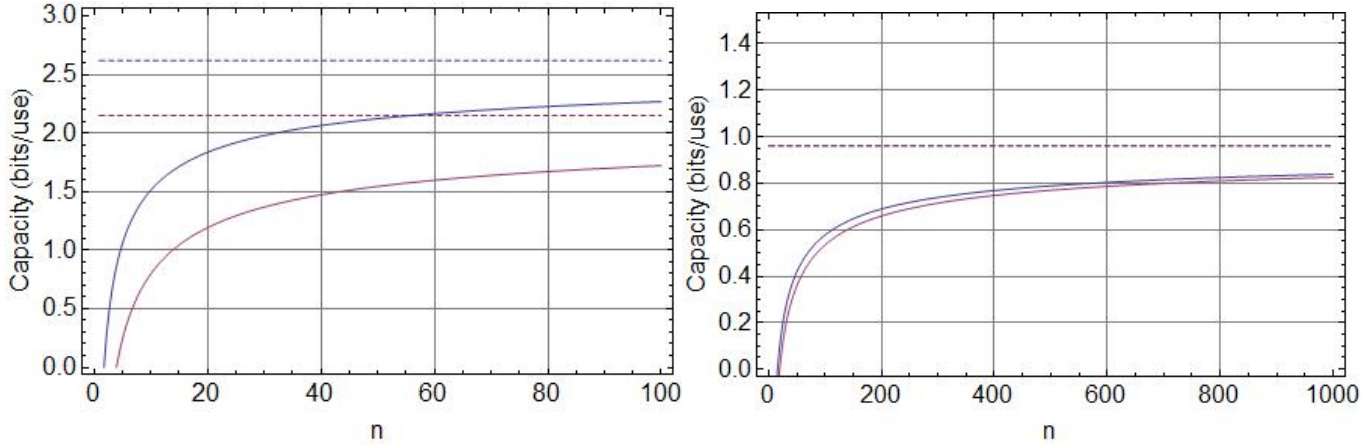


FIG. 4: Capacity (dotted curves) and finite block length capacity (solid curves) for the SWN and heterodyne receivers versus block length n. The first plot shows $M = 8$ at $N_0 = 0.8$ where the SWN has a clear advantage. The second shows $N_0 = 0.1$ which is very near the cross-over point where neither recievers has much advantage. $\epsilon = 10^{-6}$ in these plots.

I. ACKNOWLEDGMENT

[1] R.S. Bondurant, "Near-quantum optimum receivers for the phase-quadruture coherent-state channel", Optics Letters **18**, 1896-1898 (1993).

[2] R. Nair, S. Guha, and Si-Hui Tan, "Realizable receivers for discriminating arbitrary coherent-state waveforms and multi-copy quantum states near the quantum limit", Phys. Rev. A **89**, 032318 (2014).